FortiOS® 5 Wireless LAN Controller

Secure Wireless LAN Access

Fortinet Secure Wireless LAN Controllers are powered by FortiOS, a purpose-built network security operating system, which forms the foundation of the FortiGate Network Security Platform. Delivering the industry's most comprehensive suite of security, wireless and networking services, this enterprise class Wireless LAN Controller is purpose-built to leverage the hardware acceleration provided by custom FortiASIC™ processors. Fortinet Secure Wireless LAN Controllers deliver an easy to use and high performance enterprise wireless solution, in a single unified platform.

End-to-End Wireless LAN Security

Today's organizations are facing numerous challenges as the network environment evolves with the rapid adoption of BYOD, demanding mobile workforce and evolving security threats. The need for secure wireless networks with intra-SSID privacy, robust third-party certified security and advanced networking capabilities, is now more important than ever. Fortinet Secure Wireless LAN Controllers with FortiAP Access Points meet the demanding needs of enterprise Wireless LAN, with proven market leading security and management for both wired and wireless networks.

Unbeatable flexibility to meet all deployment needs

A wireless infrastructure must be flexible and scalable. By consolidating security and wireless network capabilities, Fortinet Secure Wireless LAN Controllers significantly reduce network complexity and ultimately TCO. Fortinet's no-VLANs™ approach reduces complex Layer-2 requirements, eliminating the need to propagate VLAN information across the network to simplify and accelerating large, scalable deployments.

Key Features and Benefits

Scalable and Resilient	Highly scalable and centrally managed enterprise WLAN, with integrated radio resource management to reduce co-channel interference and provide consistent WLAN performance.
Integrated UTM Features	Extends wired security features to WLAN, unifying both wired and wireless management into a single console, providing a "Single Pane of Glass" management interface to the network.
Layer-7 Application Visibility	Leverage the market leading UTM features with the power of ASIC-based deep packet inspection technology to deliver granular application level visibility and control.

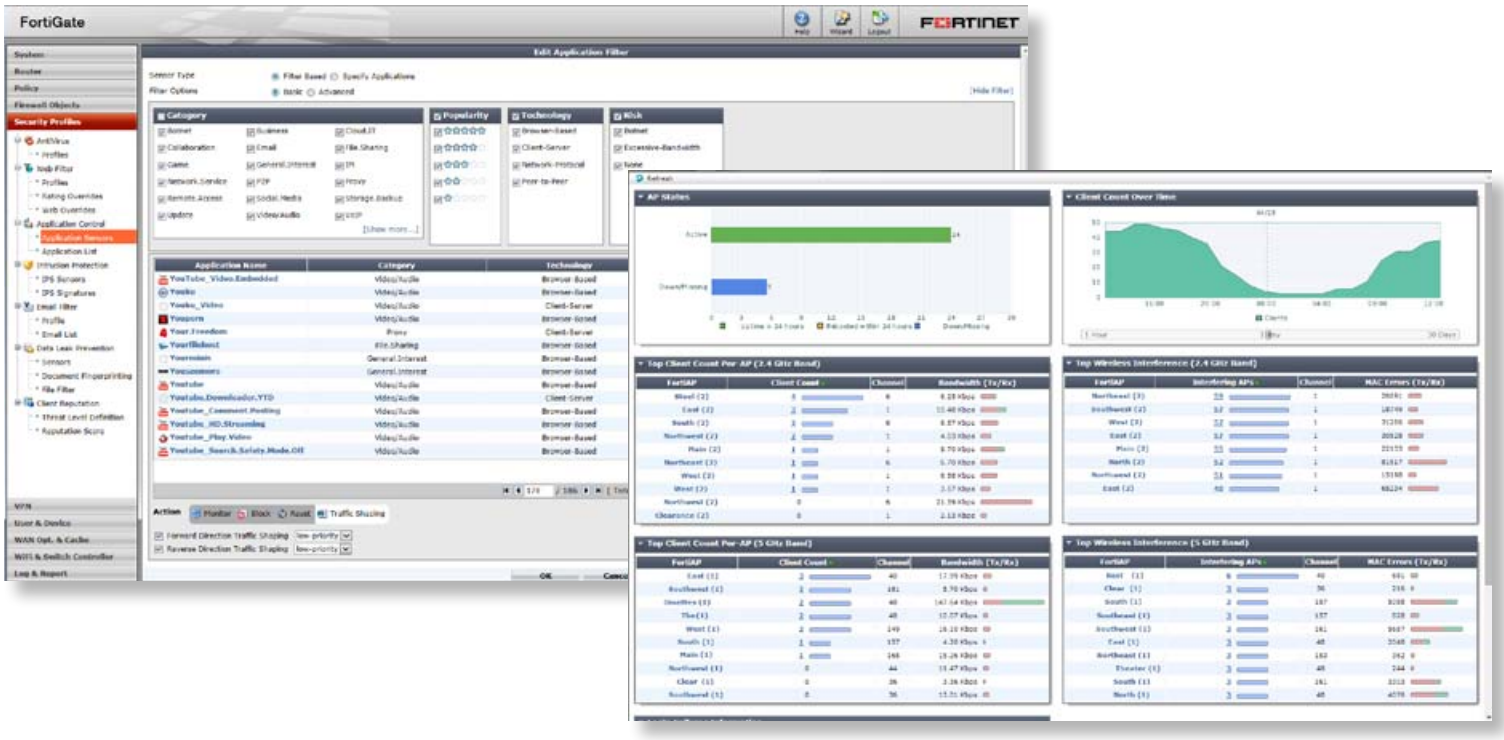
FortiOS 5 Wireless LAN Controller Highlights

- True Enterprise WLAN System
- Support for 802.11ac Gigabit WiFi
- Flexible Deployment Models for Distributed Enterprise, Education, Healthcare and Hospitality
- Integrated UTM Security and Management
- Automatic Radio Resource Provisioning
- PCI Compliance Capabilities for Retail Stores
- Integrated Guest Access Management with Captive Portal
- BYOD Device Finger Printing and Control
- Deep Layer-7 Application Control
- Easy to use Centralized Management through Web GUI
- Multi-Hop Mesh
- Point-to-Point Bridging
- Remote AP with Cloud Controller
- Integrated WIDS and Rogue AP Management
- Scale from 1 to 10,000+ of APs

ICSA labs CERTIFIED

Wi Fi CERTIFIED

HIGHLIGHTS



FortiOS Web-based GUI — Application Control and Wireless Health Dashboard

Single pane of glass management

Integrating wired and wireless security into a single pane of glass lowers operating costs and reduces IT staff workloads by eliminating the complexities of troubleshooting a multivendor network and the need for costly training and certification across multiple vendor products. In addition to reducing operating costs, a single pane of glass for management also ensures that a consistent security and control policy is applied across both the wired and wireless networks.

Sophisticated Application Control

Wireless bandwidth is a precious shared medium and it is critical that business applications receive priority on the wireless LAN. FortiOS Application Control is built-in to the Wireless LAN controller and uses deep Layer-7 inspection with over 2,700 application signatures to provide bandwidth guarantees and prioritization of critical applications. This industry leading Application Control capability provides the fine-grained application control required to ensure the Wireless LAN is performing at its best and is being utilized for the intended applications.

Industry Leading Security

FortiOS has its pedigree in Unified Threat Management and Fortinet holds more industry certifications than any other vendor, providing the best-in-class unified protection with an integrated set of security services. From antivirus, web content filtering, application control, network IPS, email filtering and DLP, the same security that is applied to the wired network can now be applied to the wireless LAN.

Built-in Wireless Intrusion Detection System capabilities intelligently further protects the wireless LAN by detecting a vast array of RF intrusion techniques including:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking

HIGHLIGHTS

Automated Rogue AP Detection and Suppression

Rogue access points pose a serious network security threat by creating a leakage point where sensitive data such as credit card information can be siphoned off the network. For this reason, the PCI DSS and other data security standards often mandate proactive monitoring and suppression of rogue APs. The FortiGate Rogue AP on-wire detection engine uses various correlation techniques to determine if a Rogue AP is connected to the network. This automated process continuously monitors for unknown APs and automatically suppress any found to be unauthorized.

High Density

FortiOS monitors wireless client connections on each AP and ensures the connection load is spread uniformly across the network. This ensures better airtime utilization and provides increased capacity, resulting in a better performing WLAN. Devices can also be distributed across radios (frequencies) on a single AP, by intelligently steering dual band devices to the less crowded and higher performance 5 GHz band.

Automatic Radio Resource Provisioning

FortiOS DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.

Strong, Flexible Authentication

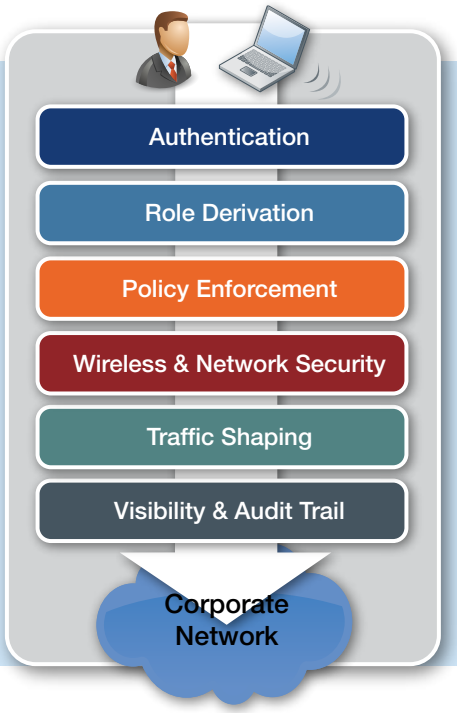
FortiOS supports standard WPA2 authentication using pre-shared keys as well as enterprise grade authentication using 802.11i or 802.1x with RADIUS. When 802.1x is enabled, users are authenticated against a backend RADIUS server, either provided by FortiAuthenticator or directly against a Microsoft Active Directory server. FortiOS also supports embedded public certificates for WPA-Enterprise authentication, MAC address authentication and MAC address white/black lists for complete and flexible authentication options based on the network constraints.

Guest Captive Portal

Browser-based authentication for guest users is also supported in using via the SSL enabled captive portal. This built-in captive portal allows for HTML login page customization as well as guest account provisioning and management via an integrated guest management portal. FortiOS also supports universal access method (UAM) for integrating with third-party external captive portal servers as well as two-factor authentication with the FortiToken One Time Password (OTP) solution.

Wireless LAN Planning and Analysis

FortiPlanner is a graphical Wireless LAN Planning and Post-Deployment Site Survey utility, designed to simplify WLAN planning and deployment of Fortinet FortiAP based wireless networks. Sophisticated signal propagation ray tracing algorithms are used to ensure precise pre-deployment planning accuracy, as well as accurate post-deployment visualization via real-time heat-maps.



Secure Wireless LAN

Complete Secure Wireless LAN architecture:

- Captive Portal, 802.1x, Temporary Guest Access
- User & Device Identification, Authorization
- User & Device based policies, Application Control
- Rouge AP Mitigation, Wireless Intrusion Detection
- User & Application Based Wireless QOS
- Detailed Network & Threat Visibility, Compliance Reporting

FEATURE SUMMARY

WIRELESS CONTROLLER

Networking

DHCP	Integrated DHCP server
VLANs	Interface and trunk
	SSID to VLAN mapping
	Dynamic VLAN Support
Routing	Static, dynamic and policy routing
	RIP, OSPF and BGP support
Multicast	PIM Mode
	Multicast to unicast conversion
Data Forwarding	Centralized – Tunneled to FortiGate, no VLANs
	Distributed – Bridged locally
	Split Policy Based – Selective forwarding based on resources, policy

Provisioning and Management

Management Access	HTTPS via web browser
	SSH, Telnet and console
	SNMP (V1 and V2)
Monitoring	Access Point (radio, channel) – Status, usage, utilization
	Client monitoring – Signal strength, SNR, username, IP, device type, firewall policy, bandwidth usage, application visibility
	Rogue AP
	Mesh connectivity hierarchy
	Wireless health monitoring, client trends, overloaded APs, excessive RF errors
Centralized Management	Single pane of glass management for wired and wireless security and configuration
	Centralized management of thousands of locations via FortiManager
	Centralized reporting, network analytics and trends of thousands of locations via FortiAnalyzer
Troubleshooting	Remote wireless packet capture

Remote AP

Remote AP Support	Supported on all FAP models
	Enables FAPs to be deployed remotely (over WAN link) to the FortiGate Wireless LAN Controller
	Option to encrypt data traffic via DTLS
	Split routing – Selective forwarding based on policy (FortiOS 5.2)
WAN Survivability	Wireless client connectivity is maintained when the wireless controller is unreachable for open and PSK type SSIDs
Troubleshooting	Local FAP diagnostic web portal

Mesh and Bridging

Topology	Multi-hop mesh
	Support for multiple mesh instances
Mesh Hops	Configurable maximum hop count
Bridging	Point-to-Point bridging
	Point-to-Multipoint bridging for wireless ISP applications
Management	Via FortiGate web interface

Wireless Access and Authentication

Access – Authentication Methods	IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA)
	RFC 2716 PPP EAP-TLS
	RFC 2865 RADIUS authentication
	RFC 3579 RADIUS support for EAP
	RFC 3580 IEEE 802.1x RADIUS Guidelines
	RFC 3748 Extensible Authentication Protocol
	WEP64 – 64-bit Web Equivalent Privacy
	WEP128 – 128-bit WEP
	WPA (Wi-Fi Protected Access) Personal and Enterprise
	WPA2 (Personal and Enterprise) – 802.11i standard
	MAC address authentication
	MAC address authentication via RADIUS
	Certificate based authentication for BYOD
Authentication Servers	Internal Database, RADIUS, LDAP, TACACS+
	External Authentication Servers – Microsoft Active Directory, Microsoft IAS RADIUS server, Cisco ACS Server, FreeRADIUS , Interlink RADIUS server, Steel Belted Radius
Encryption Protocols	CCMP/AES
	TKIP
	TKIP+AES
	DTLS
	L2TP/IPSec (RFC 3193)
	XAUTH/IPSec
VPN	SSL
	IPSec
Captive Portal	Authentication against internal or external authentication server
	Fully customizable look and feel including branding, graphics and language
	Disclaimer page
	Multiple-captive portal pages
	Forward to external captive portal (FortiOS 5.2)
	Redirect to website after authentication (FortiOS 5.2)
Guest User Management	Integrated receptionist guest user management portal
	Configurable expiration time
	Configurable start times
	Bulk account creation
	Integration with FortiAuthenticator for self-service captive portal with e-mail login

RF and Performance Management

DAARP (Distributed Automatic Radio Resource Provisioning)	Automated selection of RF channel to achieve consistent optimal performance
DAARP Scheduling	Configurable (enable/disable)
	Enable with the option to exclude time slots
802.11n HT20 and HT40 support	Supported
802.11ac 80 MHz option	Supported on 802.11ac models
Band Steering	Load-balances stations across 2.4 GHz and 5 GHz RF bands for optimal performance and reducing interference
AP Load Balancing	Distribute clients evenly across APs on available channels
Self Healing	Automatically adjust TX power levels to extend coverage to compensate failed APs
RF Planning	Enabled by FortiPlanner software
	Predictive RF planning
	Real-time Dynamic Heatmaps
	Site Survey

Rogue AP Management

Background Scanning	Background and full-time scanning for rogue APs
On-Wire Correlation	On-Wire correlation to identify malicious APs that are connected to the local network
Rogue Suppression	Configurable options for automatic and/or manual suppression options
	Over-the-air suppression of offending APs and counter measures to prevent clients attempting to connect to an identified rogue AP
Wireless IDS	Detects and logs multiple RF intrusion methods
Event Logging	Syslog of all Rogue AP events
Auditing	Pre-built reported for PCI-DSS compliance generated via FortiAnalyzer

BYOD and Mobility

Device Identity	Distinguish between corporate assets and employee owned devices
	Identify and classify device types, vendor information, OS types and OS versions
Application Visibility	Layer-7 application detection with support for over 3,000 signatures
	Ability to detect, prioritize or suppress applications
Quality of Service	End-to-end QoS
	Policy based retagging of applications
	Preserve QoS tags across the wired and wireless network
	Prioritize transmission of business critical applications over wireless

FEATURE SUMMARY

Policy Management	Manage and enforce firewall and traffic shaping policies based on device and user identity
Mobility Support	Fast Roaming — 2–3ms between APs on the same FortiGate
	802.11i fast-roam back
	802.11i fast-associate in advance
	PMK caching
Presence Detection	Presence detection for presence analytics
IPv6 Support	
Client Support	Support for IPv6 clients
Management	Management over IPv6 — Support for FortiGate to act as IPv6 node
Traffic	Routing protocols, firewall and UTM support
Certifications	
Wi-Fi Alliance	Wi-Fi Alliance certified (802.11a/b/g/n/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Save).
Firewall	ICSA firewall enterprise certification
	ICSA IPv6 certified firewall
	USGv6 certified firewall
IEEE Standard Compliance	802.11a, 802.11b, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (UAPSD), 802.11n with HT40 support, 802.11ac
	802.11e and WME/WMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues
	802.11h, 802.11j
	802.11i (TKIP/AES), 802.1x

NOTE: Feature set based on FortiOS Version 5.2. Unique FortiOS 5.2 features are marked, some features or certification may not apply to all models.

FORTIAP	
Operation Modes	Access Point
	Full-time Monitor
	Mesh root
	Point to Point Bridge Mode
	Stand-alone Site Survey mode
Controller Discovery	Static IP
	Automatic discovery via Multicast AND Broadcast
	Pre-provisioned AP using Serial No
	DHCP Option 138
	DNS FQDN discovery
	Up to 3 controllers addresses kept in memory

ADDITIONAL REFERENCES

Resources	URL
The FortiOS Handbook — The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
FortiAP Website	http://www.fortinet.com/products/fortiap/index.html
Product Datasheets and Matrix	http://www.fortinet.com/resource_center/datasheets.html
Secure WLAN Solution Page	http://www.fortinet.com/solutions/wireless.html

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480